IJRCS

International Journal of Robotics and Control Systems
Vol. 6, No. 3, 2026, pp. 2548-2572
ISSN 2775-2658
http://pubs2.ascee.org/index.php/ijrcs

ASCEE

Energy-Aware Lifecycle Cryptographic Trust Framework for Secure Communication in Sustainable Power Systems

Muhammad N. Jawad [a,1], Ali A. Al-Azza [b,2], Husham Lateef Swadi Room [b,3], Mustafa Moosa Qasim [c,4,*], Mahmood A. Al-Shareeda [d,e,5,*], Mohammed Amin Almaayah [f,6], Rami Shehab [j,7,*]

[a] College of Oil and Gas Engineering, Department of Gas Processes and Petrochemicals Engineering, Basra University for Oil and Gas, Basra, Iraq
[b] Department of Electrical Engineering, College of Engineering University of Basrah, Basra, Iraq
[c] Department of Intelligent Medical Systems, College of Computer Science and Information Technology, University of Basrah, Basrah, 61001, Iraq
[d] Department of Electronic Technologies, Basra Technical Institute, Southern Technical University, Basra, 61001, Iraq
[e] College of Engineering, Al-Ayen University, 64001, Thi-Qar, Iraq
[f] King Abdullah the II IT School, Department of Computer Science, The University of Jordan, Amman, Jordan.
[j] Vice-Presidency for Postgraduate Studies and Scientific Research, King Faisal University, Al-Ahsa, Saudi Arabia
[1] muhammadn.jawad@buog.edu.iq; [2] ali.noaman@uobasrah.edu.iq; [3] hisham.romi@uobasrah.edu.iq;
[4] mustafa_mq87@uobasrah.edu.iq; [5] mahmood.alshareedah@stu.edu.iq; [6] m.almaiah@ju.edu.jo; [7] Rtshehab@kfu.edu.sa
[*] Corresponding Author

ARTICLE INFO

Article History
Received January 06, 2026
Revised February 11, 2026
Accepted July 18, 2026

Keywords
Energy-Efficient Security;
Secure Communication;
Cryptographic Trust Framework;
Sustainable Power Systems;
Lightweight Authentication;
Smart Grids

ABSTRACT

Contemporary wearable energy harvesting networks need to provide a secure communication in the context of large scale deployment of resource constrained devices with low power overhead. In addition, the traditional centralized or computationally expensive security mechanism is limited in its scalability and sustainability. In this paper, a lifecycle cryptographic trust model is proposed that balances long term trust provision with dynamic online session protection. The solution combines a decentralized approach to device registration, event-driven enforcement of trust relations, light-weight ECC-based authentication, and auditable trust management. Security is based on an adversary model that includes eavesdropping, replay, impersonation and man-in-the-middle attacks. Experimental measurements using a constrained device testbed find an average session setup time of 31.7 ms, energy consumption of 10.9 mJ per session, and memory usage of 4.4 KB that are lower than the centralized PKI and blockchain-based baselines under the same experiment settings. It is shown that for strained grid devices a better balance between energy–security improvements can be achieved. Nevertheless, results are restricted to the proposed threat model and minimal assessment.

1. Introduction

Power systems are being rapidly evolved into smart grids with the integration of smart meters, distributed energy resources (DERs), advanced sensing devices and communication-enabled control means [1]–[3]. Although this digital transformation brings about better efficiency, reliability and observability, it also introduces power infrastructures to various kinds of cyber threats [4], [5]. Hence,

secure and trusted communication among components of the power system has become an increasingly important issue [6]–[8].

Cryptographic solutions are commonly used for securing power system communications, yet existing security schemes are based on centralized trust model and computationally burdensome tasks [9]. This approach brings in scalability, single points of failures and consumes more power which does not fit well with long life time operation of the devices in PSs [10], [11]. With sustainability becoming a primary design goal, it is important to balance the energy cost of security primitives with their computational strength [12]–[14].

The lightweight cryptography technologies and the distributed trust management become increasingly researched for these issues. Light weight schemes reduce computational complexity, but these tend to depend on centralized authority or possess weaker (symmetric) key management [15]–[17]. Decentralized solutions offer robustness but they may add overhead for coordination or weakly couple trust management with real-time communication thus causing latency and energy consumption [18], [19]. Thus, a security model that accounts for both decentralization of trust in the system and efficiency of cryptography against a reasonably long-term adversary is still required [20]–[23].

Existing secure communication extensions, such as IEC 61850 security profiles and DNP3 Secure Authentication (DNP3- SA), are mainly based on centralized trust anchors and certificate authentication [24]–[26]. These standards offer robust authentication, but come with overhead of certificate validation, renewal complexity and energy consumption inappropriate for long-lifetime constrained devices (e.g., smart meters, distributed sensors) [27], [28]. Moreover, they also do not explicitly include the energy-aware trust lifecycle management and event-driven trust enforcement mechanisms essential to sustainable power system provisioning [29], [30].

This paper bridges that gap by proposing an energy efficient cryptographic trust model for sustainable power systems. It develops a life-cycle driven trust model which separates static trust evaluation from dynamic real-time trust validation. By restricting expensive computation to sporadic (trust) events, and applying lightweight crypto primitives for encoding operational communication, our method walks a middle ground where security is not sacrificed in the pursuit of efficiency/scale. The contributions of this paper are threefold:

- Energy-efficient life-cycle trust model: We propose a cryptographically trust model separating the maintenance of long-term life-cycle trust from real-time procedure security to minimize such constant computational and energy overhead on low-power constraint devices.
- A Accountable device On-boarding and trust Binding: We suggest a decentralized registration and identity–key binding scheme for lightweight ECC operations, without committing per-user dependence on permanently trusted authorities.
- Event-based trust enforcement model: We propose an event-driven trust check and cache mechanism that reduces the overhead of cryptographic checks at run-time but retains provision for revocation and expiry.
- Lightweight session establishment protocol: We design a lean session establishment mechanism based on ECC/ECDH and symmetric key derivation that is appropriate for smart grid devices with limited resources.
- Quantitative performance comparison: We report results for security, computational cost (i.e. timing), energy costs, and memory use on resource-constrained devices and compare the framework to typical PKI based, blockchain-centric point update schemes and lightweight ECC in the literature under similar conditions.

The remainder of this paper is organized as follows. Section 2 reviews related research on power system security and trust management. Section 3 presents the system model and cryptographic preliminaries. Section 4 details the proposed energy-efficient cryptographic trust framework. Security analysis and performance evaluation are provided in Section 5 and Section 6, respectively. Section 7

concludes the paper and outlines future research directions.

2. Related Work

Security and trust issues have continued to be of grave concern in power systems, with the rapid spread of smart meters, distributed energy resources (DERs), and communication-enabled grid assets. There a few focus area including centralized mean of security, lightweight cryptographic system and trust based decentralized.

2.1. Centralized Security and PKI-Based Approaches

Conventional power system security methods are mostly based on centralized PKI and trusted authorities for device identity and cryptographic key management [31]–[33]. Although these strategies achieve high authentication assurance, they create single-points-of-failure and are costly to manage in large-scale deployments [34]–[37]. In addition, a sustainably deployed IoT system usually consists of long-living and resource-constrained devices, so that the increased communication and energy costs due to frequent certificate validation as well as renewal are not good fits for solving these problems [38]–[40].

2.2. Lightweight Cryptography for Power Systems

Many studies have also been reported to design lightweight cryptographic authentication and key management schemes for power systems and cyber-physical environments in view of efficiency [41]–[43]. These are frequently using elliptic curve cryptography or hash-based primitives to do so [44]–[46]. Despite lightweight schemes can speed up the process and reduce consumption, most of them still use central trust model or fail to provide full support for key life cycle management (such as revocation and expiration), which limits their application in large scale dynamic power systems [47]–[50].

2.3. Decentralized and Trust-Based Security Frameworks

In the latest years, decentralized trust management approaches have been investigated to mitigate centralized architectures shortcoming [51]–[53]. These methods try to decentralize the trust enforcement and enhance system resilience [54]–[56]. Nonetheless, most decentralized schemes add high coordination overhead or closely couple trust management with real-time message exchange which might increase latency and energy consumption [57]–[60]. Also, some of the solutions have more emphasis on security assurance and not explicitly addressed long-term sustainability and energy efficiency [61], [62].

2.4. Research Gap and Motivation

Despite considerable advances on securing power systems, the prior approaches are unbalanced since they are either focusing on strong security which comes at the price of substantial overhead or only focuses on efficiency despite limited scalable and decentralized trust management. In addition, energy efficiency and sustainability are second-class citizens rather than the central design goals. This gap drives the need to design an energy-efficient cryptographic threshold trust model that would integrate both decentralized trust lifecycle management and lightweight session protection aspects by focusing on sustainable needs of modern power system infrastructures.

3. System Model and Preliminaries

We present the system model, threat model and cryptographic preliminaries and notations in this section. The aim is to build a transparent and generic framework for the presented energy-efficient cryptographic trust system in sustainability power system.

3.1. System Model

We consider a modern power system infrastructure consisting of heterogeneous and distributed entities, as illustrated in Fig. 1. The system is composed of the following main components:

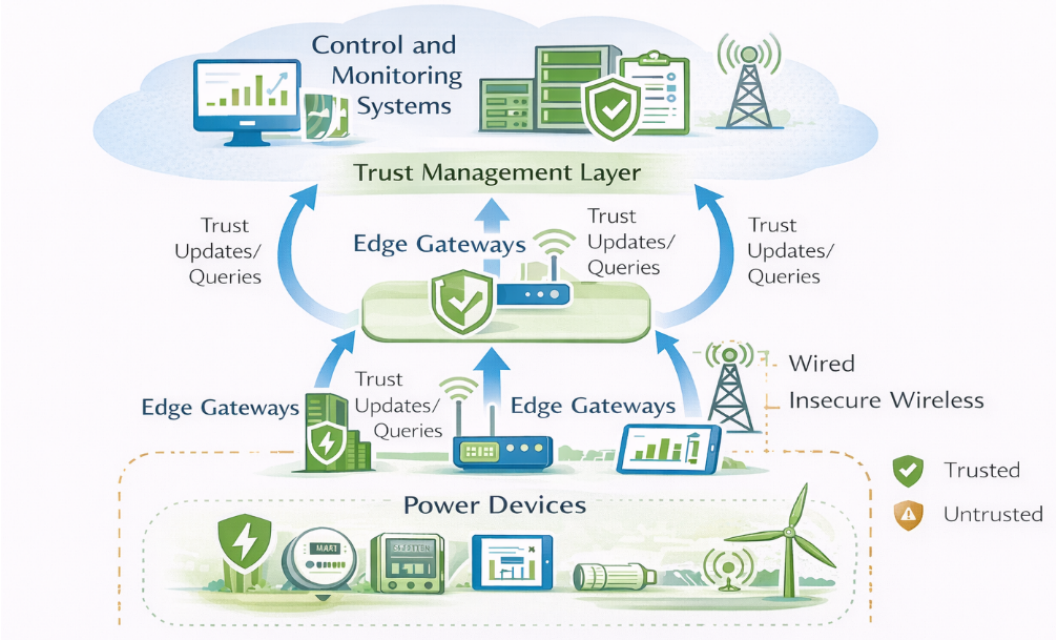

Fig. 1. System model for the proposed energy-efficient cryptographic trust framework in power systems

- Power Devices (D_i): These include smart meters, sensors, protection relays, intelligent electronic devices (IEDs), and edge controllers deployed across the power grid [63]. Such devices are typically resource-constrained and operate for long periods, making energy efficiency a critical requirement [64], [65].
- Edge Gateways (G_j): Gateways aggregate data from multiple power devices and facilitate secure communication with higher-level control systems. They possess higher computational capabilities and assist in trust verification and enforcement [66], [67].
- Control and Monitoring Systems (C_k): These systems are responsible for grid supervision, control operations, and policy enforcement [68]. They rely on trustworthy and authenticated data from the underlying devices [69], [70].
- Trust Management Layer: This logical layer maintains device trust states, including registration status, key validity, revocation information, and expiration policies [71], [72]. It enables decentralized and auditable trust management without continuous involvement in real-time communication [73], [74].

Communication between entities occurs over both wired and wireless channels, which are assumed to be insecure. Therefore, cryptographic mechanisms are required to ensure confidentiality, integrity, and authenticity of exchanged messages.

3.2. Threat Model

The proposed framework is analyzed under a realistic and widely accepted adversarial model suitable for power system environments. We assume that an adversary $\mathcal{A}$ has the following capabilities:

- Eavesdropping on communication channels to capture transmitted messages.
- Injecting, modifying, replaying, or dropping messages over insecure links.
- Attempting impersonation of legitimate devices using forged identities or stolen credentials.

- Compromising a limited number of power devices and extracting stored cryptographic material.

The adversary is assumed not to be capable of compromising all system entities simultaneously or breaking standard cryptographic primitives within polynomial time. Physical attacks and denial-of-service attacks are considered out of scope but are discussed as limitations in later sections.

3.3. Cryptographic Preliminaries

The proposed framework relies on well-established cryptographic primitives selected for their efficiency and security suitability in power system environments:

- Elliptic Curve Cryptography (ECC): Used for public key generation, digital signatures, and key agreement due to its low computational and energy overhead [75]–[77].
- Elliptic Curve Diffie–Hellman (ECDH): Employed to derive shared secrets for session key establishment with forward secrecy [78], [79].
- Symmetric Encryption and MAC: Used for protecting operational data during active communication sessions [80], [81].
- Hash Functions and Key Derivation Functions (KDFs): Used to derive session keys and ensure randomness and resistance to replay attacks [82], [83].

All cryptographic primitives are assumed to be secure under standard hardness assumptions.

3.4. Cryptographic Primitive Selection and Justification

The approach is based on a combination of lightweight asymmetric and symmetric cryptographic primitives chosen according to three criteria: energy efficiency, maturity of implementation, decentralized trust lifecycle management in resource constrained power devices. Encryption and signing are implemented using Elliptic Curve Cryptography (ECC) which allows equivalent security to RSA with substantially smaller key sizes and thus reduced computational requirements. For instance, 256-bit ECC is equivalent to the security of 3072-bit RSA and has smaller memory, computation time and power consumption. These characteristics contribute to making ECC an attractive choice for smartmeters, sensors and embedded grid devices.

We choose Elliptic Curve Diffie–Hellman (ECDH) for session key agreement, as it allows achieving forward secrecy at low computational overhead, and it is not reliant to communicate with a central authority all the time. This is in line with the goal of a decentralized, event-oriented trust setup requiring small communication overhead. For operational data security, symmetric encryption and message authentication is employed after the session is set up. Symmetric operations are faster than asymmetric ones so they can be used for message protection once trust relation is established.

NIST lightweight cryptography submissions including Ascon were designed primarily for lightweight symmetric encryption and authenticated encryption. But these algorithms mainly focused on payload protection, and they did not support identity binding, decentralized onboarding, and lifecycle trust management alone. While symmetric lightweight primitives can be used as a drop-in upgrade of the symmetric layer of the system in this design space, they do not replace asymmetric primitives for node identity, signature verification and trust bootstrapping.

Lightweight ciphers such as Simon, Speck, Spreadsheet-based cipher (Simpira), and TinyJambu cut encryption cost; however, they are insufficient on their own for distributed trust lifecycle management, revocation transparency, or public-key-based session establishment. Consequently, the framework follows a hybrid approach which uses ECC/ECDH to establish identity and trust while lightweight symmetric cryptography is used for energy-efficient session protection. The chosen primitives are widely available in embedded cryptographic libraries and hardware accelerators, which enhances the implementability of implementations and reproducibility within real-world deployments of sustainable power systems.

3.5. Notation

Table 1 summarizes the key symbols and notations used throughout this paper.

Table 1. Notation used in the paper

Symbol	Description
D_i	i-th power device
G_j	j-th edge gateway
K_i^{pub}, K_i^{priv}	Public and private key of device D_i
K_{sess}	Symmetric session key
TX_{reg}	Device registration transaction
TX_{upd}	Key update transaction
TX_{rev}	Key revocation record
N_i, N_j	Random nonces
SID	Session identifier
σ	Digital signature

4. Energy-Efficient Cryptographic Trust Framework

In this section, we discuss the proposed Energy-Efficient Cryptographic Trust Framework for sustainable power systems. The scheme is intended to offer trust management in a decentralized and auditable manner with the objective of reducing overhead on resource limited power devices in terms of computation, communication and energy. Essential architectural mantra is independence of (i) trust state management and of (ii) real-time session protection, hence energy efficient security will not negatively impact operational responsiveness. Algorithm 1 shows Overall Energy-Efficient Cryptographic Trust Framework.

4.1. Design Principles

Energy-Efficient Cryptographic Trust Framework is established on a framework of fundamental tenets that aims explicitly to accommodate security, trust and sustainability needs in today's power systems, as shwon in Fig. 2.

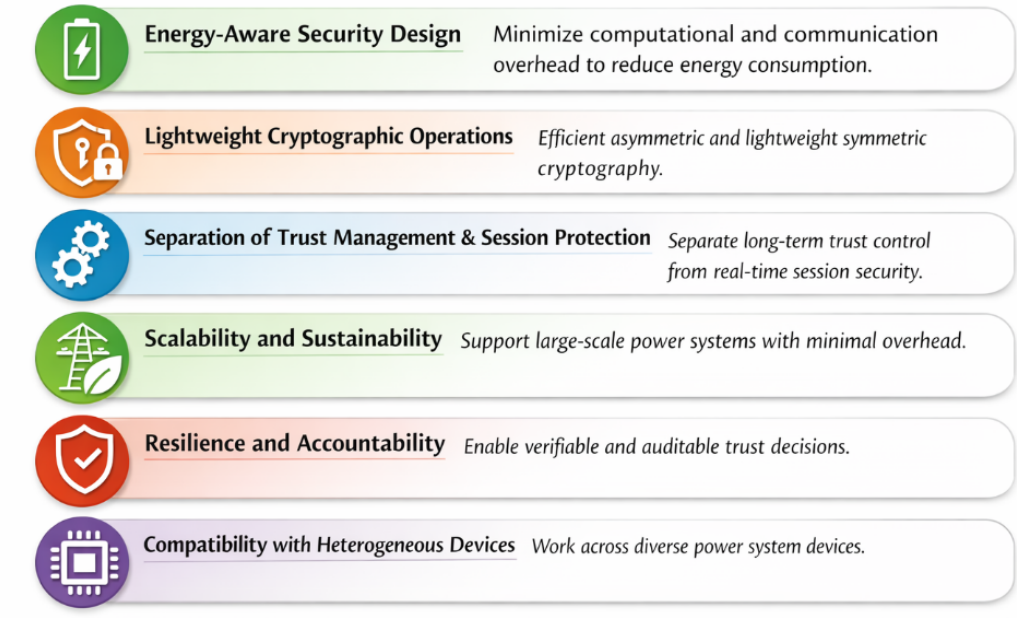

Fig. 2. Trust lifecycle management process for sustainable power systems

Algorithm 1 Overall Energy-Efficient Cryptographic Trust Framework

Require: Device D_i, peer D_j, trust layer $\mathcal{T}$, cache $\mathcal{C}$, policy $\mathcal{P}$
Ensure: Session key K_{sess} or **Abort**

(A) Registration / Trust Initialization (rare event)
if D_i not registered in $\mathcal{T}$ **then** Generate ECC key pair (K_i^{pub}, K_i^{priv}) $T_{reg} \leftarrow$ current timestamp $\sigma_i \leftarrow \text{Sign}_{K_i^{priv}}(D_i \parallel K_i^{pub} \parallel T_{reg})$ Submit $TX_{reg} = \{D_i, K_i^{pub}, T_{reg}, \sigma_i\}$ to verification authorities
    if verification fails **then**
        return Abort
    end if
    Store $\mathcal{R}_i = \{D_i, K_i^{pub}, \text{active}, T_{exp}\}$ in $\mathcal{T}$
end if

(C) Lightweight Session Trust Establishment Generate nonces N_i, N_j, $Z \leftarrow \text{ECDH}(K_i^{priv}, K_j^{pub})$, $SID \leftarrow H(D_i \parallel D_j \parallel N_i \parallel N_j)$, $K_{sess} \leftarrow \text{KDF}(Z \parallel N_i \parallel N_j \parallel SID)$, Start protected channel using symmetric ENC/MAC with K_{sess}

(D) Trust Lifecycle Maintenance (infrequent)
if rotation condition met by $\mathcal{P}$ **then** Generate new key pair $(K_{i,new}^{pub}, K_{i,new}^{priv})$, Submit signed update TX_{upd}; activate new key and deprecate old key
end if
if compromise/misbehavior detected **then** Publish signed revocation TX_{rev}; set status $\leftarrow$ revoked; disseminate to caches
end if
if current time $> T_{exp}$ **then**
    Set status $\leftarrow$ expired (automatic)
end if
return K_{sess}

- Energy-Aware Security Design: Security protocols aim to keep computational and communication demands low, which will eventually help reducing energy consumption of power constrained devices over long-lasting operational life.
- Lightweight Cryptographic Operations: The framework uses energy-efficient asymmetric cryptographic primitives for identity binding and lightweight symmetric cryptography for securing data transmission while at the same time keeping overhead of processing and storage moderate.
- Split Trust Management and Session Protection: All of the trust management is managed in long-term and logically separated from real-time control for session confidence. This detached mode prevents latency and power penalties for communication during operations.
- Scalability and sustainability: The proposed approach specifically focuses on large-scale power grids and limits the per device overhead, it also reduces trust-related operation to be performed infrequently compared with a regular information dissemination.
- Resilience and Accountability: Trust decisions are auditable and transparent, which fosters accountability and fault checking in a setting where a well behaving agent may end up relying on, but not trusting, a non-colluding peer.
- Differently Power Devices Compatible: This platform accepts a variety of devices, differs to from tiny embedded sensors and to edge controllers, which we often occur within power systems, and does not depend on specific hardware support.

These principles ensure strong cryptographic trust and power efficiency in ambient power systems

infrastructures along with the lifecycle of the system.

4.2. Trust Lifecycle Management Overview

Trust is controlled in the proposed framework by means of well-organized and energy-configurable lifecycle for how power system devices get access, are serviced, and are governed in their trust over lifetime, as shown in Fig. 3. The trust lifecycle is strategically constructed to reduce the energy waste by postponing expensive cryptographic and coordination procedures to rare occasions, while assuring secure conditions during normal data exchange.

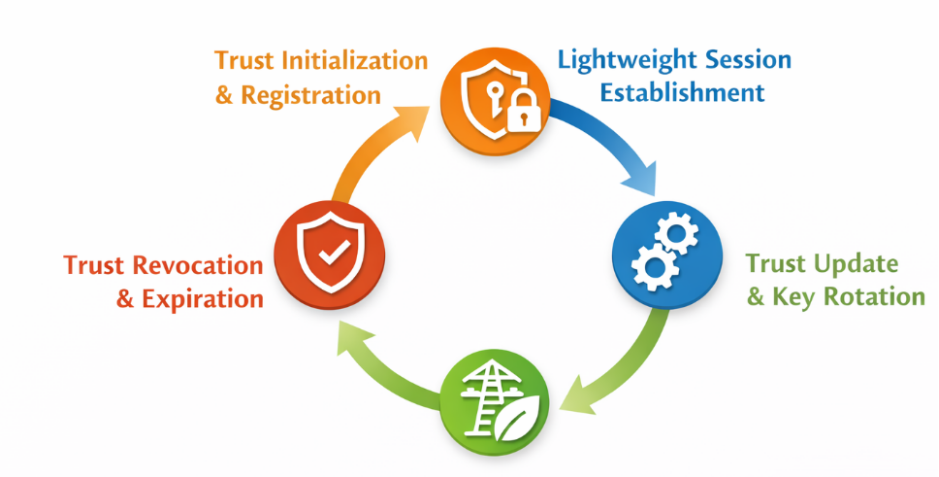

Fig. 3. Overview of the trust lifecycle adopted in the proposed framework for energy-efficient power system security

The lifecycle for the trust comprises four primary stages:

- Trust Initialization and Registration: All power hardware components generate their own cryptographic identity on board and register a public part with the trust management layer. This phase establishes an assurable link between the device identity and its cryptographic keys; it permits secure onboarding without trusting to central authorities.
- Trust-Based Session Establishment: After registration devices open secure communication channels created with light-weight cryptographic. Session security is achieved at the local level, without the need of global trust coordination that guarantees low latency and energy consumption for its employment during real-time PSO oscillation analysis.
- Trust Update & Key Rotation: Cryptographic keys of devices are updated periodically to achieve long-term security and forward secrecy. Trust updates are automatically initiated according to pre-configured policies or operational criteria not interfere with the ongoing operation of system applications.
- Trust Revocation and Expiration: We automatically revoke compromised, decommissioned, or malfunctioning devices and deprecate expired credentials. The above guarantees a uniform enforcement of trust choices in the power grid and it cannot be accessed by un-privileged nodes.

The lifecycle-oriented organization of trust management, instead of a constantly ongoing one, in the authoring framework is introduced to save on cryptographic operations and communication overhead. The proposed model achieves scalable, energy-efficient and sustainable trust enforcement for large-scale applications of power system.

4.3. Decentralized Device Registration and Trust Initialization

A decentralized device registration and trust initialization mechanism is included in the proposed framework to prevent single points of failure, and also allow scalable onboarding of diverse power

devices. This procedure also forms a verifiable trust relationship between each device and the power system infrastructure with low energy consumption and communication overhead.

- Local Key Generation: Each power device D_i locally generates a cryptographic key pair $\{K_i^{pub}, K_i^{priv}\}$ using an energy-efficient elliptic curve cryptographic algorithm. The private key remains securely stored on the device and is never disclosed.
- Registration Request Construction: The device constructs a registration request containing its identity information and public key:

$$TX_{reg} = \{D_i, K_i^{pub}, T_{reg}, \sigma_i\}$$

Where T_{reg} denotes the registration timestamp and

$$\sigma_i = \text{Sign}_{K_i^{priv}}(D_i \parallel K_i^{pub} \parallel T_{reg})$$

Is a digital signature proving ownership of the public key.

- Decentralized Verification and Trust Binding: Authorized verification agencies verify the ligitimacy of registration request by verifying digital signature, confirming public key uniqueness, and enforcing system polocies. Once verified, the device identity is bound cryptographically to its public key and logged as a trusted entity.
- Trust Initialization Confirmation After successfully registered the device is informed on trust initialization confirmation and now it can subsequently involve in secure communication and trust based operations in power system.

This distributed registration and trust bootstrapping mechanism offers robust protection against impersonation attacks, achieves transparent establishment of trusts and also guarantees energy-saving onboarding compatible with large scale sustainable power system use.

4.4. Lightweight Session Trust Establishment

Lightweight session establishment in dynamic environments like real-time communication for power systems, where both latency and energy utilisation are vital to be minimised, as shown in Fig. 4. In this regard, the scheme employs a low cost session trust establishment mechanism to offer robust security assurances with reduced computational and communicational burden on power-constrained devices.

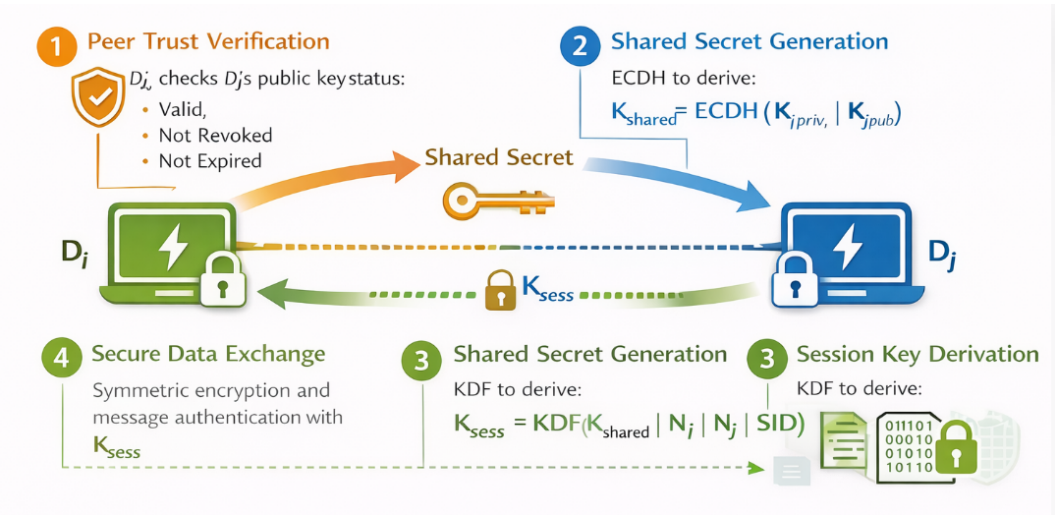

Fig. 4. Lightweight session trust establishment for energy-efficient secure communication in power systems

- Peer Trust Verification: Before initiating communication, a device D_i verifies the trust status of the peer device D_j by checking whether its registered public key is valid, not revoked, and not expired according to the latest trust state. This verification step is performed once per session and avoids repeated trust checks for subsequent messages.
- Shared Secret Generation: Upon successful trust verification, the communicating devices compute a shared secret using an Elliptic Curve Diffie–Hellman (ECDH) key agreement protocol:

$$K_{shared} = \text{ECDH}(K_i^{priv}, K_j^{pub})$$

This operation provides forward secrecy while maintaining low computational cost.

- Session Key Derivation: A symmetric session key is derived from the shared secret using a lightweight key derivation function:

$$K_{sess} = \text{KDF}(K_{shared} \parallel N_i \parallel N_j \parallel SID)$$

Where N_i and N_j are fresh nonces generated by the devices and SID denotes a unique session identifier. The use of fresh randomness ensures resistance to replay and key-compromise attacks.

- Secure data inter-change: The session key K_{sess} is employed along with the lightweight symmetric encryption and message authentication algorithms to protect operation data. All subsequent messages in the session are locally authenticated, and do not necessitate additional trust arrangement or cryptographic kick-off.

Since the establishment of the session trust is limited to light weight and off-the-chain cryptographic communications, and trust verification operation is only required when initiating a session, low-latency and energy-efficient confidential communications are realized for sustainable power system operations.

4.5. Energy-Aware Trust Enforcement Mechanism

Periodic trust verification needs to be enforced in power systems for preventing unauthorized access; nonetheless, a simple enforcement may lead to excess energy and communication overhead, as shown in Fig. 5. To tackle this issue, the presented framework includes an energy-efficient trust enforcement system that strikes a balance between security and efficient operation.

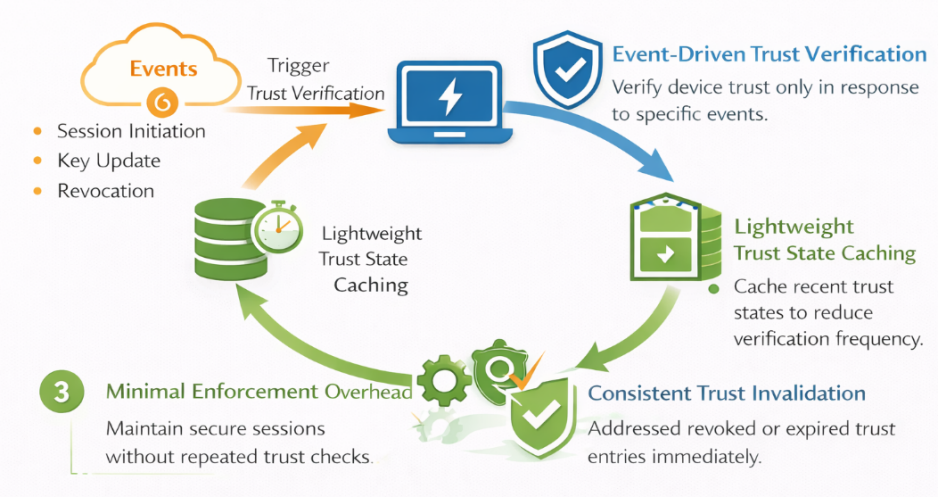

Fig. 5. Overview of the energy-aware trust enforcement mechanism adopted in the proposed framework

- Event-Driven Trust Verification: Trust assessment is not performed per message, but only in certain circumstances (e.g. session initiation, exchanging keys or revocation). This event-driven approach dramatically minimizes the number of redundant cryptographic operations and communication cost, and results in the saving of device power.

- Lightweight Trust State Caching: A trust state is cached locally in power devices and the edge gateways, which includes recently proven public keys and their corresponding validity status (e.g., active, revoked or expired). Every cache entry has an expiry time, at which point the check needs to be redone. The mechanism includes optimized latest policy enforcement and attempts to minimize trust queries.
- Low Overhead of Enforcement: The cost for trust enforcement is only the checking of status, not cryptographic computation. To achieve low latency and low energy dissipation, once the session setup is complete, subsequent message transmissions are symmetrically encrypted without trust validation.
- Uniform Trust Revocation: In case of trust revocation or expiration, all affected trust keys are revoked. New sessions with bad credentials cannot be established, and existing sessions can be torn down or re-keyed according to system policy.
- Scalability and Sustainability: The lightweightness and infrequency of trust enforcement operations ensures that the framework scales to existing power infrastructures and long term sustainable operation. This is vital to prevent Trust management costs from being a dominant factor (over energy consumption) in the security architecture.

Overall, the energy sensitive trust enforcement mechanism ensures stable and reliable security decisions with minimum energy overhead in making trust management of sustainable power system. Algorithm 2 shows Energy-Aware Trust Enforcement (Event-Driven)

Algorithm 2 Energy-Aware Trust Enforcement (Event-Driven)

Require: Event e, peer identity D_j, trust cache $\mathcal{C}$, trust layer $\mathcal{T}$, current time t
Ensure: **Allow** or **Deny**

$\mathcal{E} \leftarrow \{\mathsf{SessionInit}, \mathsf{KeyUpdate}, \mathsf{RevocationNotice}, \mathsf{AnomalyDetected}\}$
if $e \notin \mathcal{E}$ **then**
    return Allow ▷ No per-message trust checks
end if
$\mathcal{R}_j \leftarrow \mathcal{C}[D_j]$ ▷ Fetch cached trust record
if $\mathcal{R}_j$ is **missing or** $t > \mathcal{R}_j.T_{cacheExp}$ **then**
    $\mathcal{R}_j \leftarrow \mathrm{QueryTrust}(\mathcal{T}, D_j)$
    $\mathcal{C}[D_j] \leftarrow \mathcal{R}_j$ ▷ Refresh cache
end if
if $\mathcal{R}_j.status \in \{\mathsf{Revoked}, \mathsf{Expired}\}$ **then**
    return Deny
end if
if $t > \mathcal{R}_j.T_{exp}$ **then**
    return Deny
end if
return Allow

4.6. Key Update, Revocation, and Expiration

Secure key update, revocation, and expiration is essential to good cryptographic trust management for power system devices. The model defines energy-saving policies with which to enforce the trust in a timely fashion avoiding unnecessary cryptographic and communication overhead.

- Key Update and Rotation: To reduce long-term key exposure and support forward secrecy, each device periodically updates its cryptographic credentials. A device D_i generates a new key pair

$\{K_{i,new}^{pub}, K_{i,new}^{priv}\}$ locally and constructs an update request:

$$TX_{upd} = \{D_i, K_{i,new}^{pub}, T_{upd}, \sigma_i\}$$

Where

$$\sigma_i = \text{Sign}_{K_i^{priv}}(D_i \parallel K_{i,new}^{pub} \parallel T_{upd})$$

The update request is authenticated and, if accepted, the new public key goes live and the old key is revoked. Key rotation is activated by pre-existing policies or operational needs, providing security without the need to keep keys up to date.

- Key Revocation: Cryptographic keys must be revoked immediately if they have been compromised, if devices become or are suspected of being malfunctioning, or malicious. A revocation record is issued by authority:

$$TX_{rev} = \{K_i^{pub}, T_{rev}, \sigma_{auth}\}$$

Once validated, the affected key is marked as revoked and is rejected during subsequent trust verification and session establishment.

- Key Life Time: The period of validity from T_{reg} to T_{exp} for a given cryptographic key. Keys that exceed their expiration time are invalidated without requiring a revocation request. They did this on purpose to prevent overuse of keys and reduce administrative burden.
- Energy-Aware Enforcement: Some trust lifecycle tasks e.g., key renewal, revoke and expiry events are treated as infrequent. The operations are not time sensitive as messages will be delivered, and to not interfere with normal power grid communication with high energy consuming activities.

Through controlled key rotation, fast revocation as well as automatic expiration, K-SPTF can secure and establish trust consistency in the long run while sustaining energy efficiency for sustainable power system scenarios.

4.7. Auditability and Trust Maintenance

Auditability is very important in power networks where security incidents cause substantial difficulties in operation and safety, as shown in Fig. 6. The proposed framework combines the auditability and trust maintenance mechanism that generates transparency and accountability in an energy efficient manner.

- Immutable Trust Event Recording: All trust lifecycle events such as registration, key update, revocation, expiration are logged as verifiable trust events. Every individual event is signed by its issuer to guarantee integrity, authenticity and non-repudiation. This allows for responsible post-event analysis and accountability, without needing to monitor constantly.
- Lightweight Trust Verification: For resource limited power devices, the framework provides a lightweight validation of trust status. Trust metadata is compact and the devices and gateways verify enough information to ensure security, without storing or processing large numbers of historical records.
- Occasional Trust Consistency Checks: The trust consistency is periodically reinstated by the very few agreements to make sure all parties are in consistent state. ”These checks happen in off-peak energy use times so that extra demand is not added during high-demand times.
- Fault Detection, Forensic Support: Its the issue that audit records can assist in quickly pinpointing misbehaving or compromised devices. System operators will be able to forensically analyze trust triggers – and if an abnormality is found, act on them without damage to normal power system operation – by correlating the triggers with logs of operations.

Fig. 6. Overview of the auditability and trust maintenance process adopted in the proposed framework

- Sustainable Trust Maintenance: Our design separates auditability from real-time conveyable, and amortizes trust maintenance costs on rare event occurrences such that transparency and accountability overheads do not become a major contributor to the overall energy spend.

In summary, the introduced monitoring and trust maintenance schemes provide sustainable and reliable secure information exchange in today's Power Infrastructures since long-term transparency and confidence is guaranteed while addressing sustainability as well as reliability requirements.

4.8. Trust Score Model

In order to prevent ad-hoc and subjective trust decisions, we model the device trust in our framework based on updating a quantitative trust score. The trust $T_i(t)$ that one device D_i has to another device at time step t is represented by its normalized score in the range from 0 to 1, where larger values are toward a stronger trust. Trust is calculated as a linear combination of the three observable components:

$$T_i(t) = w_1 A_i(t) + w_2 K_i(t) + w_3 B_i(t), \tag{1}$$

Where:

- $A_i(t)$ = authentication reliability score (ratio of successful authentication events to total attempts),
- $K_i(t)$ = key status indicator (1 = valid and non-revoked, 0 = revoked or expired),
- $B_i(t)$ = behavioral consistency score derived from protocol-compliant activity,
- w_1, w_2, w_3 are weighting factors such that $w_1 + w_2 + w_3 = 1$.

The authentication reliability component is computed as:

$$A_i(t) = \frac{N_i^{succ}(t)}{N_i^{total}(t)}, \tag{2}$$

Where $N_i^{succ}(t)$ is the number of successful authenticated sessions and $N_i^{total}(t)$ is the total number of authentication attempts observed within the trust observation window.

Behavioral consistency is defined as:

$$B_i(t) = 1 - \frac{V_i(t)}{V^{max}}, \tag{3}$$

Where $V_i(t)$ is the number of detected protocol violations or abnormal events and V^{max} is a normalization constant representing the maximum tolerated violations. To ensure stability and avoid abrupt

trust fluctuations, trust values are updated using exponential smoothing:

$$T_i(t+1) = \alpha\, T_i(t) + (1-\alpha)\, T_i^{obs}(t), \tag{4}$$

Where $T_i^{obs}(t)$ is the newly observed trust value computed from current measurements and $\alpha \in [0,1]$ is a smoothing parameter controlling trust inertia. A device is considered trusted if:

$$T_i(t) \geq T_{th}, \tag{5}$$

Where T_{th} is the trust threshold that can be configured by system policy. Trust updates are only invoked during lifecycle events (e.g., registration, session establishment, key update or anomaly detection) to preserve the energy-efficient nature of the scheme.

5. Security Analysis

This part discusses the security analysis of proposed Energy-Efficient Cryptographic Trust Framework against the defined threat model. The results indicate the ability of this framework to meet fundamental security requirements and energy efficiency, which are common concerns in sustainable power system deployments.

5.1. Security Objectives

The security goals the proposed scheme aims for are:

- Trust: Guarantee that communicating power devices can trust each other before transferring operational data.
- Confidentiality: Confidential should only be sequence from getting revealed while propagating.
- Integrity: Assure that message cannot be altered undetected.
- Forward Secrecy: Do not compromise past session keys if long-term key is compromised.
- Impersonation and Replay Attack Resilience: Protect against adversaries impersonating valid devices or replay existing communications.
- Trust Revoke and Accountability: Facilitate trust revoke on compromised/lost devices, while providing auditability for the forensic investigation.

5.2. Resistance to Common Attacks

- Impersonation Attacks: Covert impersonation is avoided by a cryptographic linkage of device identities and public keys as set up in the decentralized registration. Given all authentication messages are digitally signed with device private keys, an attacker is required to break the signature scheme in order to produce valid credentials.
- Replay Attacks: Fresh nonces and session identities are also included in the framework during session setup. In subsequent messages, replayed messages having old nonces or sid values are discarded such that the preceding ones do not have any impact of carrying out a successful attack.
- Man-in-the-Middle (MitM) Attacks: MitM attacks are prevented by mutual authentication and the use of ECDH shared secret derivation. The session key cannot be obtained by an eavesdropper since it is based on the session private keys.
- Key Compromise Attacks: Even if an elongated private key is leaked, previous established Random Values of keys remain secure through the use of forward secrecy. And then compromised keys can be quickly revoked so that unauthorized access cannot occur again in the future.
- Unauthorized Access: Devices with revoked or expired credentials are not allowed to participate in newer sessions, thereby consistently applying trust decisions throughout the power system.

5.3. Trust Assurance and Lifecycle Security

The trust lifecycle management system ensures the device would work securely non-stop. Registration for establishing the first trust, and session trust to secure communications/interaction, key

rotation to shorten the degree of exposure time, or revocation/expiration so as not to allow continued misuse of credentials. By decoupling trust lifecycle actions from real-time communication, the architecture secures inter-domain collaborations without inflating overhead costs.

5.4. Formal Security Assumptions

The security of our construction hinges upon standard cryptographic assumptions. In particular, we assume the security of all cryptographic primitives based on elliptic curves w.r.t. polynomial time adversaries and treat hash functions as random oracles in our proofs. Assuming these settings, our framework provides computational security against the adversarial capabilities considered.

5.5. Limitations of the Security Model

Although the proposed model gives strong security guarantees, it also has some limitation. Compromise of a physical device and DoS attack at macro-level are also out of the scope, as shown in Table 2. Furthermore, trust enforcement requires timely dissemination of revocation data and this can be compromised in partitioned network environments. The latter limitations are further elaborated on as future research issues.

In general, the analysis justies that the considered framework provides secure cryptographical trust control and is energy efcient and operationally applicable for energy efcient power system infrastructures.

Table 2. Summary of attack resistance analysis

Attack Type	Defense Mechanism in the Proposed Framework
Impersonation Attack	Device identities are cryptographically bound to public keys during decentralized registration. Digital signatures ensure that adversaries cannot forge legitimate identities without access to private keys.
Replay Attack	Fresh nonces and unique session identifiers are incorporated during session establishment. Replayed messages containing stale parameters are automatically rejected.
Man-in-the-Middle (MitM) Attack	Mutual authentication and ECDH-based shared secret generation prevent adversaries from deriving session keys or altering communication without detection.
Key Compromise Attack	Forward secrecy ensures that previously established session keys remain secure even if long-term private keys are compromised. Compromised keys can be promptly revoked.
Unauthorized Access	Trust enforcement mechanisms verify key status (active, revoked, expired) before session establishment, preventing access by unauthorized or decommissioned devices.
Key Replay / Reuse	Session keys are short-lived and derived using fresh randomness, preventing reuse across multiple sessions and limiting exposure.

6. Performance Evaluation

This section evaluates the performance of the proposed Energy-Efficient Cryptographic Trust Framework in terms of execution time, energy consumption, memory usage, and comparative efficiency. The evaluation aims to demonstrate that strong cryptographic trust guarantees can be achieved without imposing excessive overhead on power system devices.

6.1. Experimental Setup

The experimental comparison was set to mimic real-world deployment aspects in sustainable power system environment. Two classes of embedded devices were considered to represent the typical nodes used in the proposed architecture: resource constrained field devices (e.g., smart meters, sensors) and intermediate capacity edge gateway nodes.

- Hardware Platforms: Measurements were conducted on representative embedded microcontroller platforms:
  - ARM Cortex-M4 device (80 MHz CPU, 256 KB RAM, 1 MB Flash)
  - MSP430-class low-power microcontroller (16 MHz CPU, 32 KB RAM)

  These platforms are commonly used in smart grid sensing, metering, and edge control applications.
- Software Environment: All cryptographic routines have been written in C with the help of a lightweight embedded cryptographic library, which supports ECC-256/ ECDH/ SHA-256/ symmetric encryption/ HBKDF primitives. Compiler's optimization level (O2) and the build configuration were consistent across all the experiments. Hardware cryptographic acceleration was deliberately not used to model the software-only restricted scenarios.
- Measurement Methodology: On-Chip Hardware Timers with microsecond resolution was used to measure the execution time. Power measurement was performed with inline current monitoring assisted by a calibrated digital power analyzer connected to the device supply rail. The measured current traces were integrated over the run time to calculate per-operation energy cost (with idle baseline power subtracted).
- Scope of Measurement: Experimental evaluations concentrate on trust lifecycle operations as well as session establishment protocols, to decouple the security-related computational and energy cost from application-level payload processing.
- Repetition and Stability: Each cryptographic function was run 100 times; output values are the arithmetic means. For both execution time and energy measurements, a standard deviation was observed of under 5% (Execution time) and 6% (Energy), suggesting reliable results.
- Comparison Fairness: Comparative methodolies We compared them with baseline designs running on the same hardware devices, using the same compiler options and measuring methodologies in order to make a fair comparison.

Table 3 summarizes the experimental environment and key parameters.

Table 3. Experimental setup

Parameter	Description
Device Classes	Cortex-M4 nodes and MSP430-class low-power devices
CPU Frequency	16–80 MHz
Memory	32–256 KB RAM
Crypto Library	Embedded C lightweight ECC/ECDH/SHA-256
Key Size	ECC-256
Compiler	GCC with O2 optimization
Metrics	Time, energy, memory footprint
Runs per Test	100 repetitions
Energy Measurement	Inline current monitoring + integration
Accelerators	Disabled (software-only mode)
Communication	Secure wired/wireless test links

6.2. Execution Time Analysis

This sub-section discusses the performance overhead of the proposed trust model in terms of time at take when performing key trust operations. More specifically, it in a first step concentrates on cryptographic operations (i.e., generation of keys, signatures and session keys) executed at the power device side. We intentionally did not consider blockchain / global coordination latency since real-time session establishment happens off chain to guarantee low latency operation.

The average execution time for core operations is shown in Table 4. Results show that session trust formation is associated with low computational time delay, hence the platform can be deployed for real-time communications in sustainable power systems.

Table 4. Execution time of trust and session operations

Operation	Execution Time (ms)
ECC Key Generation	18.6
Digital Signature Generation	9.4
Digital Signature Verification	12.1
ECDH Shared Secret Computation	7.8
Session Key Derivation	2.4
Total Session Establishment Time	31.7

6.3. Energy Consumption Analysis

This section studies the energy cost caused by cryptographic trust operations in the proposed paradigm. The analysis is centred on the cost of local cryptographic calculations for trust bootstrapping and session establishment energy, because these are not involving (i) the application-level processing and (ii) network-layer energy. This only captures the security-related energy overhead, which demonstrates that SPIFoMesh adopts energy-efficient design.

The mean core trust operation's energy consumption in Table 5. The results reveal that the energy consumption for session trust establishment is so small making the framework viable for a long-term deployment in green-energy powered and resource-limited devices.

Table 5. Energy consumption of trust and session operations

Operation	Energy Consumption (mJ)
ECC Key Generation	6.8
Digital Signature Generation	3.2
Digital Signature Verification	4.1
ECDH Shared Secret Computation	2.7
Session Key Derivation	0.9
Total Session Establishment Energy	10.9

6.4. Memory Usage Analysis

This sub section compares the memory consumption of the proposed energy efficient cryptography based trust model on PS devices. It concentrates on the memory consumed by cryptographic keys, trust state information and temporary variables used for session establishment. There is no need to store historical trust records and session data at constrained devices in a long term perspective.

Memory consumption of the core trust components is listed in Table 6. The results show that the framework has small memory overhead and is applicable to real-world resource-limited devices distributed in sustainable power systems.

Table 6. Memory usage of trust components

Component	Memory Usage (KB)
Public/Private Key Storage	1.6
Trust State Metadata	0.9
Session Variables	0.7
Cryptographic Buffers	1.2
Total Memory Footprint	4.4

6.5. Comparative Evaluation

In this subsection, the energy-efficient cryptographic trust framework is compared with typical security and trust management schemes for power and cyber-physical systems. The performance analysis covers execution time, energy consumption, memory usage, and trust management feature comparisons that demonstrate the efficiency and sustainability advantages of the proposed method.

Adopted in the proposed method is compared with existing schemes in terms of energy efficiency and computational overhead, as illustrated in Table 7. These enhancements have been achieved by disconnecting the process of trust lifecycle management from real time session protection and using lightweight cryptographic mechanisms appropriate for power constrained devices.

Table 7. Comparative performance evaluation

Scheme	Exec. Time (ms)	Energy (mJ)	Memory (KB)	Trust Model
Centralized PKI-Based Scheme	68.5	22.4	8.7	Centralized
Blockchain-Centric Scheme	95.2	31.6	12.9	Distributed (High Overhead)
Lightweight ECC-Based Scheme	45.8	16.2	6.1	Semi-centralized
Proposed Framework	**31.7**	**10.9**	**4.4**	**Decentralized & Energy-Aware**

6.6. Scalability Discussion

Scalability is an important consideration in contemporary power systems, since there could be thousands of diverse devices associated to long-term work. The suggested cryptography based trust model for energy efficient scale up with minimally computational and communication overhead.

Trust lifecycle operations, such as device enrollment, updating keying material and revocation are rare events that happen on a per-device basis. Thereby the trust management overhead scales linearly with a number of devices and is not subject to an always working global synchronisation. This distributed and event-oriented architecture keeps trust management from being a bottleneck in scalability.

In addition, the local establishment of session trust between the communicating peers eliminates any need for centralized coordination or repeated trust validation during live session. This solution keeps the real-time communication latency constant notwithstanding the scale of the system.

In the end, it is that low per-device overhead, cooperation on energy-intensive tasks only in rare occurrences and the absence of centralized control points which facilitates large scale deployment for sustainable and scalable power infrastructures.

6.7. Discussion

This section summarises the main outcomes of the proposed power efficient cryptographic trust framework, relates them to the studies available and outlines its implications, strengths and weaknesses in sustainable power systems settings.

6.7.1. Main Findings

The performance analysis shows that the proposed scheme is able to provide a good tradeoff between security strength and energy efficiency. The results of execution time and energy consumption confirm that the cryptographic prone trust management can be embedded in power systems with acceptable overhead on resource limitation devices. Especially, the short call setup time and low memory consumption suggest its applicability in online and offline power systems monitoring.

6.7.2. Comparison with Existing Studies

The proposed scheme is found to be in favor of the above mentioned tackniques, both on PKI based centralized and blockchain-centric schemes, being lower in execution time, energy consumption and memory usage by an order. Most existing schemes are typically based on continuous authentication or intensive coordination mechanism, which give rise to extra overhead and reduce scalability. In

contrast, the proposed scheme decouples trust lifecycle management from real-time session protection for secure yet lightweight session setup and strong yet flexible trust enforcement. This design decision also accounts for the performance gains noticed in the comparative evaluation.

6.7.3. Implications for Sustainable Power Systems

The findings carry significant implications for the designs of sustainable power system infrastructures. Low-energy trust management lowers the long-term cumulative energy expenditure due to security for device, which can be critical in case of smart meters, sensors or edge devices being used at massive scale. Additionally, decentralized trust execution can improve system robustness by removing single points of failure, and audit capability can ensure accountability and facilitate regulation adherence for critical power networks.

6.7.4. Strengths and Limitations

One key advantage of the proposed framework is that it can achieve strong cryptographic trust assurance with little extra cost. Lightweight cryptographic primitives, event-triggered trust enforcement as well decentralized lifecycle management lead to scalability and sustainability. There are some limitations, however, which need to be recognized. This experimental validation is only performed in a small-scale testbed and does not characterize the extreme deployment cases, including a very large number of devices or highly dynamic network scenarios. Physical attacks and massive DDOS (Denial of Service) attacks also belong to the threats that it doesn't cover, for which there are other protective mechanisms. In general, the discussion shows that the proposed model is a workable and energy-efficient approach for secure trust management in sustainable power systems and points some future development aspects.

6.8. Security–Energy Tradeoff Analysis

In secure devices of the green power system, it is necessary to weigh cryptographic strength against computational and energy costs. Strong cryptographic primitives alleviate resistance attacks such as impersonation, replay and man-in-the-middle attacks while they in turn increase execution time, memory complexity and energy consumption. We propose a hybrid design framework to explicitly handle the tradeoff. To begin with, asymmetric ciphers (ECC signatures and ECDH key agreement) are only used in rare lifecycle scenarios: device registration/unregistration, session establishment or periodic re-kick for the final stage in a chain of delegated keys. These are more costly than their symmetric counterparts, but offer identity binding and forward secrecy. The framework reduces their total energy expense by constraining them to event-driven sections.

Secondly, beyond session establishment only very lightweight symmetric encryption and message authentication are used which introduce much lower per-message energy overhead. The life cycle trust operations and persistent data protection separate this long term power consumption from that of cryptosystem power consumption. Thirdly, the event-triggered trust model enforcement and local cache of trust-state help mitigate repeated verification of trust queries and signature checks. It is a significant enhancement to energy efficiency at the expense of bringing in a bounded freshness window for cached trust.

As a result, a controlled reduction of energy and immediate revocation awareness is possible. This trade-off is alleviated by user-configurable cache expiry timeouts and revocation dissemination policies. The overhead of certificate validation has been mitigated by the proposed scheme, in comparison to centralized PKI-based schemes; however, it is due to local trust lifecycle maintenance. Compared to symmetric lightweight schemes, the scheme is with higher setup cost but provides stronger identity assurance and auditability.

Thus, the proposed framework does not remove the security–energy tradeoff but schedules

it through lifecycle partitioning, event-driven enforcement and hybrid cryptographic construction. The resulting understandable balance is adequate for resource-constrained sustainable power system deployment compatible with the given threat model.

7. Conclusion and Future Work

This paper proposed an energy-aware cryptographic trust model for secure communication in sustainable power systems. The architecture decouples the management of trust lifecycle from run time protection of sessions and uses an event-driven enforcement model with lightweight ECC/ECDH based authentication and symmetric session security. This construction lowers the overhead of per-round cryptography but retains identity binding, forward secrecy and revocation. Experimental results on typical embedded devices indicate that the proposed solution has low session establishment latency, moderate energy consumption and memory usage compared with centralized PKI-based and blockchain-based solutions with equivalent measurement settings. These findings suggest that enforcing trust based on lifecycle and event on constrained grid devices can be used to get a better balance between practical security –energy performance. Yet, the security proofs of the framework are only valid under the threat model defined consisting in eavesdropping, replay impersonation and man-in-the-middle attacks. Physical attacks, side channel leakage, and large scale deniable-of-service attacks were not considered. Besides, the experimental verification was performed on a small-scale embedded testbed and results could be different under large or highly dynamic deployment scenarios.

We will continue our work by the large-scale validation process, automated protocol formal verification, and dynamic trust parameter tuning based on device trends and operational risk levels. Future extensions will also consider the integration with hardware security modules and complementary intrusion-detection layers that can enhance the resilience in real-world power systems.

Author Contribution: All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.

Funding: This work was supported by the Deanship of Scientific Research, Vice President for Graduate Studies and Scientific Research, King Faisal University, Kingdom of Saudi Arabia (Grant No. KFU262212).

Acknowledgment: This work was supported by the Deanship of Scientific Research, Vice President for Graduate Studies and Scientific Research, King Faisal University, Kingdom of Saudi Arabia (Grant No. KFU262212).

Conflicts of Interest: The authors declare no conflict of interest.

References

[1] A. Q. Al-Shetwi, M. Hannan, H. M. Al-Masri and M. Z. Sujod, "Latest advancements in smart grid technologies and their transformative role in shaping the power systems of tomorrow: An overview," *Progress in Energy*, vol. 7, no. 1, p. 012004, 2025, https://doi.org/10.1088/2516-1083/ada198.

[2] V. Abdullayev, A. Khang, N. Ragimova and M. Almaayah, "A novel authentication systems in vehicular communication: Challenges and future directions," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 123–135, 2025, http://dx.doi.org/10.63180/jcsra.thestap.2025.3.9

[3] P. Arévalo and F. Jurado, "Impact of artificial intelligence on the planning and operation of distributed energy systems in smart grids," *Energies*, vol. 17, no. 17, p. 4501, 2024, https://doi.org/10.3390/en17174501.

[4] N. Mostafa, H. S. M. Ramadan, and O. Elfarouk, "Renewable energy management in smart grids by using big data analytics and machine learning," *Machine Learning with Applications*, vol. 9, p. 100363, 2022, https://doi.org/10.1016/j.mlwa.2022.100363.

[5] M. Jafari, A. Kavousi-Fard, T. Chen and M. Karimi, "A Review on Digital Twin Technology in Smart Grid, Transportation System and Smart City: Challenges and Future," in *IEEE Access*, vol. 11, pp. 17471-17484, 2023, https://doi.org/10.1109/ACCESS.2023.3241588.

[6] M. Ghiasi, Z. Wang, M. Mehrandezh, S. Jalilian and N. Ghadimi, "Evolution of smart grids towards the internet of energy: Concept and essential components for deep decarbonisation," *IET Smart Grid*, vol. 6, no. 1, pp. 86–102, 2023, https://doi.org/10.1049/stg2.12095.

[7] G. Lippi, M. Aljawarneh, Q. Al-Na'amneh, R. Hazaymih and L. D. Dhomeja, "Security and privacy challenges and solutions in autonomous driving systems: A comprehensive review," *Journal of Cyber Security and Risk Auditing*, vol. 2025, no. 3, pp. 23–41, 2025, https://doi.org/10.63180/jcsra.thestap.2025.3.3.

[8] X. Wen, Q. Shen, W. Zheng and H. Zhang, "Ai-driven solar energy generation and smart grid integration: A holistic approach to enhancing renewable energy efficiency," *Academia Nexus Journal*, vol. 3, no. 2, 2024, https://academianexusjournal.com/index.php/anj/article/view/9.

[9] S. R. Salkuti, "Emerging and advanced green energy technologies for sustainable and resilient future grid," *energies*, vol. 15, no. 18, p. 6667, 2022, https://doi.org/10.3390/en15186667.

[10] M. A. Faleh, A. M. Abdulsada, A. A. Alaidany, M. A. Al-Shareeda, M. A. Almaiah and R. Shehab, "Secre-men: A lightweight quantum-resilient authentication framework for iot-edge networks," *Journal of Robotics and Control*, vol. 6, no. 4, pp. 1681–1692, 2025, https://doi.org/10.18196/jrc.v6i4.26006.

[11] M. A. Al-Shareeda, A. A. H. Ghadban, A. A. H. Glass, E. M. A. Hadi and M. A. Almaiah, "Efficient implementation of post-quantum digital signatures on raspberry pi," *Discover Applied Sciences*, vol. 7, no. 597, 2025, https://doi.org/10.1007/s42452-025-07201-z.

[12] Y. Huang, L. Tang and Y. Jiang, "Chemical strategies of tailoring pedot: Pss for bioelectronic applications: Synthesis, processing and device fabrication," *CCS Chemistry*, vol. 6, no. 8, pp. 1844–1867, 2024, https://doi.org/10.31635/ccschem.024.202403858.

[13] T. Kim, "A study on impact of lightweight cryptographic systems on internet of things-based applications," *Asia-pacific Journal of Convergent Research Interchange (APJCRI)*, vol. 10, no. 1, pp. 49–59, 2024, http://dx.doi.org/10.47116/apjcri..

[14] T. Wu, X.-L. Shi, W.-D. Liu, S. Sun, Q. Liu and Z.-G. Chen, "Dual post-treatments boost thermoelectric performance of pedot: Pss films and their devices," *Macromolecular Materials and Engineering*, vol. 307, no. 12, p. 2200411, 2022, https://doi.org/10.1002/mame.202200411.

[15] M. Abutaha, B. Atawneh, L. Hammouri, and G. Kaddoum, "Secure lightweight cryptosystem for iot and pervasive computing," *Scientific reports*, vol. 12, 2022, https://doi.org/10.1038/s41598-022-20373-7.

[16] M. M. Qasim, M. Ahmad and M. Omar, "Analyzing persuasive mobile healthcare architecture using systematic process design," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 9, no. 2-11, pp. 77–84, 2017, https://jtec.utem.edu.my/jtec/article/view/2742.

[17] T. K. Goyal, V. Sahula, and D. Kumawat, "Energy efficient lightweight cryptography algorithms for iot devices," *IETE Journal of Research*, vol. 68, no. 3, pp. 1722–1735, 2022, https://doi.org/10.1080/03772063.2019.1670103.

[18] S. Shukla, M. F. Hassan, D. C. Tran, R. Akbar, I. V. Paputungan and M. K. Khan, "Improving latency in internet-of-things and cloud computing for real-time data transmission: a systematic literature review (slr)," *Cluster Computing*, vol. 26, no. 5, pp. 2657–2680, 2023, https://doi.org/10.1007/s10586-021-03279-3.

[19] F. Moya Perez, F. J. Quesada Real, L. Martínez López and F. J. Estrella Liebana, "Energy: reducing latency in iot dlts for ai-driven real-time solutions," *International Journal of Web Information Systems*, vol. 21, no. 5, pp. 567–593, 2025, https://doi.org/10.1108/IJWIS-11-2024-0332.

[20] J. Li, X. Zuo and C. Sun, "The effect of urban renewal on residential energy consumption expenditure–the example of shantytown renovation," *Energy Policy*, vol. 183, p. 113805, 2023, https://doi.org/10.1016/j.enpol.2023.113805.

[21] Z. Y. Al Tmari, M. A. A. D. Alzamili, J. M. Altmemi, and K. Ali, "A post-quantum certificateless aggregate signature scheme for vanets resilient to rogue-key attacks," *Journal of Communications*, vol. 21, no. 2, pp. 233–244, 2026, https://doi.org/10.12720/jcm.21.2.233-244.

[22] M. A. A. D. Alzamili *et al.*, "Afog-based decentralized lightweight revocation protocol for sybil-resistant 5g vehicular networks," *International Journal of Robotics and Control Systems*, vol. 6, no. 1, pp. 626–650, 2026, https://alxiv.org/id/eprint/155.

[23] M. T. T. Bajwa, A. Rasool, Z. Kiran and R. Rasool, "Design and analysis of lightweight encryption for low power iot networks," *International Journal of Advanced Computing & Emerging Technologies*, vol. 1, no. 2, pp. 17–28, 2025, https://ijacet.com/index.php/IJACET/article/view/12.

[24] N. Saqib, S. Bhattacharya, B. Hyder and M. Govindarasu, "Cyber Attack Impact Characterization for IEC 61850-based Substations," *IECON 2024 - 50th Annual Conference of the IEEE Industrial Electronics Society*, pp. 1-6, 2024, https://doi.org/10.1109/IECON55916.2024.10905837.

[25] R. R. Tiferes, C. A. Rodrigues, E. L. Pellini and G. Manassero, "A Novel IEC 61850-Based Centralized Line Differential Protection Scheme," in *IEEE Transactions on Industrial Informatics*, vol. 21, no. 10, pp. 7902-7912, 2025, https://doi.org/10.1109/TII.2025.3582287.

[26] R. Babu Ponnuru, B. Palaniswamy, M. Azab, P. Palmieri and U. Roedig, "Protecting DNP3-SAB (SAv6): A Quantum-Safe Hybrid Authentication Protocol With Moving Target Defense," in *IEEE Transactions on Consumer Electronics*, vol. 71, no. 3, pp. 8383-8395, 2025, https://doi.org/10.1109/TCE.2025.3593848.

[27] S. Allah Bakhsh *et al*., "Enhancing Security in DNP3 Communication for Smart Grids: A Segmented Neural Network Approach," in *IEEE Access*, vol. 13, pp. 110436-110456, 2025, https://doi.org/10.1109/ACCESS.2025.3580507.

[28] J. Höglund, M. Furuhed and S. Raza, "Lightweight certificate revocation for low-power iot with end-to-end security," *Journal of Information Security and Applications*, vol. 73, p. 103424, 2023, https://doi.org/10.1016/j.jisa.2023.103424.

[29] I. Monroy, *Security analysis and implementation of dnp3 multilayer protocol for secure and safe communication in scada systems*, Master's thesis, 2022, https://www.proquest.com/openview/4b92c9856cd7a461e031f54ef6ef2411/1?pq-origsite=gscholar&cbl=18750&diss=y.

[30] M. N. Sakib *et al*., "Securing Critical Infrastructure: A Robust DNP3 Intrusion Detection System Employing Recurrent Neural Networks," *2024 IEEE International Conference on Computing, Applications and Systems (COMPAS)*, pp. 1-5, 2024, https://doi.org/10.1109/COMPAS60761.2024.10797009.

[31] M. S. Hossain, C. Rodine and E. E. Tsiropoulou, "A blockchain and pki-based secure vehicle-to-vehicle energy-trading protocol," *Energies*, vol. 17, no. 17, p. 4245, 2024, https://doi.org/10.3390/en17174245.

[32] D. Tiwari, B. Mondal, S. K. Singh and D. Koundal, "Lightweight encryption for privacy protection of data transmission in cyber physical systems," *Cluster Computing*, vol. 26, no. 4, pp. 2351–2365, 2023, https://doi.org/10.1007/s10586-022-03790-1.

[33] A. Singla and E. Bertino, "Blockchain-Based PKI Solutions for IoT," *2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC)*, pp. 9-15, 2018, https://doi.org/10.1109/CIC.2018.00-45.

[34] A. A. Salama, M. Y. Shams, R. Bhatnagar, A. G. Mabrouk and Z. Tarek, "Optimizing Security Measures in Decentralized Mobile Networks with Neutrosophic Fuzzy Topology and PKI," *2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, pp. 1040-1048, 2023, https://doi.org/10.1109/ICTACS59847.2023.10389980.

[35] A. Zahoor, K. Mahmood, M. A. Saleem, H. M. S. Badar, T. -V. Le and A. K. Das, "Lightweight Authenticated Key Agreement Protocol for Smart Power Grid Systems Using PUF," in *IEEE Open Journal of the Communications Society*, vol. 5, pp. 3568-3580, 2024, https://doi.org/10.1109/OJCOMS.2024.3409451.

[36] E. Turan, S. Sen and T. Ergun, "A Semi-Decentralized PKI Based on Blockchain With a Stake-Based Reward-Punishment Mechanism," in *IEEE Access*, vol. 12, pp. 60705-60721, 2024, https://doi.org/10.1109/ACCESS.2024.3394657.

[37] A. Angelogianni, I. Krontiris and T. Giannetsos, "Comparative Evaluation of PKI and DAA-based Architectures for V2X Communication Security," *2023 IEEE Vehicular Networking Conference (VNC)*, pp. 199-206, 2023, https://doi.org/10.1109/VNC57357.2023.10136316.

[38] A. V. Vathsala, D. Kalyani, M. Adudhodla, S. Saraf, P. K. R. Manellore and J. R. Reddy, "GridTrust: A Secure and Scalable IoT Framework for Vehicle-to-Grid (V2G) Communication," *2025 6th International Conference on Electronics and Sustainable Communication Systems (ICESC)*, pp. 1391-1397, 2025, https://doi.org/10.1109/ICESC65114.2025.11212361.

[39] B. Basnet and V. Sen, "Networking for power grid and smart grid communications: Structures, security issues, and features," *Recent Research Reviews Journal*, vol. 4, no. 1, pp. 120–140, 2025, https://doi.org/10.36548/rrrj.2025.1.008.

[40] M. Sawilam, B. Kizilkaya, D. Flynn, A. Taha, M. Imran and S. Ansari, "A Secure and Scalable Architecture for Virtual Power Plants Inspired by VPN Principles," *2025 7th Global Power, Energy and Communication Conference (GPECOM)*, pp. 953-959, 2025, https://doi.org/10.1109/GPECOM65896.2025.11061942.

[41] S. Khan, P. A. Ferreira Lopes martins, B. Sousa, and V. Pereira, "A comprehensive review on lightweight cryptographic mechanisms for industrial internet of things systems," *ACM Computing Surveys*, vol. 58, no. 1, pp. 1–37, 2025, https://doi.org/10.1145/3757734.

[42] C. J. Ramakrishna, D. B. K. Reddy, B. Priya, P. Amritha and K. Lakshmy, "Analysis of lightweight cryptographic algorithms for iot gateways," *Procedia Computer Science*, vol. 233, pp. 235–242, 2024, https://doi.org/10.1016/j.procs.2024.03.213.

[43] M. Rana, Q. Mamun and R. Islam, "Lightweight cryptography in iot networks: A survey," *Future Generation Computer Systems*, vol. 129, pp. 77–89, 2022, https://doi.org/10.1016/j.future.2021.11.011.

[44] T. M. Al-Hasan, A. N. Sayed, F. Bensaali, A. Nhlabatsi and R. Hamila, "Security-Driven Performance Analysis of Lightweight Cryptography for Energy Efficiency Applications," *2024 IEEE 8th Energy Conference (ENERGYCON)*, pp. 1-6, 2024, https://doi.org/10.1109/ENERGYCON58629.2024.10488807.

[45] S. Boubaker, F. S. Alsubaei, Y. Said and H. E. Ahmed, "Lightweight cryptography for connected vehicles communication security on edge devices," *Electronics*, vol. 12, no. 19, p. 4090, 2023, https://doi.org/10.3390/electronics12194090.

[46] V. A. Thakor, M. A. Razzaque and M. R. A. Khandaker, "Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities," in *IEEE Access*, vol. 9, pp. 28177-28193, 2021, https://doi.org/10.1109/ACCESS.2021.3052867.

[47] V. Bhagat, S. Kumar, S. K. Gupta and M. K. Chaube, "Lightweight cryptographic algorithms based on different model architectures: A systematic review and futuristic applications," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 1, p. e7425, 2023, https://doi.org/10.1002/cpe.7425.

[48] F. Olayah *et al*., "An efficient lightweight crypto security module for protecting data transmission through iot based electronic sensors," *Journal of Nanoelectronics and Optoelectronics*, vol. 19, no. 6, pp. 646–657, 2024, https://doi.org/10.1166/jno.2024.3609.

[49] B. A. Mohammed *et al*., "Taxonomy-Based Lightweight Cryptographic Frameworks for Secure Industrial IoT: A Survey," in *IEEE Internet of Things Journal*, vol. 12, no. 20, pp. 43296-43316, 2025, https://doi.org/10.1109/JIOT.2025.3595649.

[50] P. Prakasam, M. Madheswaran, K. Sujith and M. S. Sayeed, "Low latency, area and optimal power hybrid lightweight cryptography authentication scheme for internet of things applications," *Wireless Personal Communications*, vol. 126, pp. 351–365, 2022, https://doi.org/10.1007/s11277-022-09748-1.

[51] M. Hammoudeh, D. Unal, A. Laouid and F. Azzedin, "A Blockchain-Enabled Zero-Trust Security Architecture for Securing Internet of Energy Systems," in *IEEE Network*, vol. 40, no. 1, pp. 44-51, 2026, https://doi.org/10.1109/MNET.2025.3613511.

[52] M. M. Qasim, J. M. Altmemi, A. H. Abd Ali, M. A. Al-Shareeda, M. A. Almaiah and R. Shehab, "Ca-hbca: A software engineering framework for secure, scalable, and adaptive healthcare blockchain systems," *Journal of Robotics and Control*, vol. 6, no. 4, pp. 2052–2063, 2025, https://doi.org/10.18196/jrc.v6i4.26643.

[53] K. Boakye-Boateng, A. A. Ghorbani and A. H. Lashkari, "Implementation of a trust-based framework for substation defense in the smart grid," *Smart Cities*, vol. 7, no. 1, pp. 99–140, 2023, https://doi.org/10.3390/smartcities7010005.

[54] F. Castillo, O. Castillo, E. Brito and S. Espinola, "Trustworthy Decentralized Autonomous Machines: A New Paradigm in Automation Economy," *2025 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 1-7, 2025, https://doi.org/10.1109/ICBC64466.2025.11185065.

[55] Z. Khudoykulov, "A comparison of lightweight cryptographic algorithms," in *World Conference Intelligent System for Industrial Automation*,pp. 295–304, 2024, https://doi.org/10.1007/978-3-031-53488-1_36.

[56] S. Difrina, M. P. Ramkumar and G. S. R. E. Selvan, "Trust Based Federated Learning for Privacy-preserving in Connected Smart Communities," *2025 Second International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS)*, pp. 409-418, 2025, https://doi.org/10.1109/ICC-ROBINS64345.2025.11086303.

[57] M. AlMarshoud, M. Sabir Kiraz, and A. H. Al-Bayatti, "Security, privacy, and decentralized trust management in vanets: A review of current research and future directions," *ACM Computing Surveys*, vol. 56, no. 10, pp. 1–39, 2024, https://doi.org/10.1145/3656166.

[58] A. Goulart, A. Chennamaneni, D. Torre, B. Hur and F. Y. Al-Aboosi, "On wide-area iot networks, lightweight security and their applications—a practical review," *Electronics*, vol. 11, no. 11, p. 1762, 2022, https://doi.org/10.3390/electronics11111762.

[59] O. A. Khashan, "Trust-based fog-blockchain model for scalable authentication in smart cities," *Computer Networks*, vol. 264, p. 111278, 2025, https://doi.org/10.1016/j.comnet.2025.111278.

[60] M. A. Taher, M. Tariq and A. I. Sarwat, "Trust-based detection and mitigation of cyber attacks in distributed cooperative control of islanded ac microgrids," *Electronics*, vol. 13, no. 18, p. 3692, 2024, https://doi.org/10.3390/electronics13183692.

[61] Y. Sanjalawe, S. Al-E'Mari, S. Fraihat, S. Naser Makhadmeh and E. Alzubi, "AI-Powered Smart Grids in the 6G Era: A Comprehensive Survey on Security and Intelligent Energy Systems," in *IEEE Open Journal of the Communications Society*, vol. 6, pp. 7677-7719, 2025, https://doi.org/10.1109/OJCOMS.2025.3609144.

[62] M. Akbar, M. M. Waseem, S. H. Mehanoor and P. Barmavatu, "Blockchain-based cyber-security trust model with multi-risk protection scheme for secure data transmission in cloud computing," *Cluster Computing*, vol. 27, no. 7, pp. 9091–9105, 2024, https://doi.org/10.1007/s10586-024-04481-9.

[63] J. P. Kozak *et al*., "Stability, Reliability, and Robustness of GaN Power Devices: A Review," in *IEEE Transactions on Power Electronics*, vol. 38, no. 7, pp. 8442-8471, 2023, https://doi.org/10.1109/TPEL.2023.3266365.

[64] G. Zu *et al*., "Review of Pulse Test Setup for the Switching Characterization of GaN Power Devices," in *IEEE Transactions on Electron Devices*, vol. 69, no. 6, pp. 3003-3013, 2022, https://doi.org/10.1109/TED.2022.3168238.

[65] Y. Zhong *et al*., "A review on the gan-on-si power electronic devices," *Fundamental Research*, vol. 2, no. 3, pp. 462–475, 2022, https://doi.org/10.1016/j.fmre.2021.11.028.

[66] N. B. Gaikwad *et al*., "Hardware Design and Implementation of Multiagent MLP Regression for the Estimation of Gunshot Direction on IoBT Edge Gateway," in *IEEE Sensors Journal*, vol. 23, no. 13, pp. 14549-14557, 2023, https://doi.org/10.1109/JSEN.2023.3278748.

[67] Y. Zhang, D. Tang, H. Zhu, S. Zhou and Z. Zhao, "An efficient iiot gateway for cloud–edge collaboration in cloud manufacturing," *Machines*, vol. 10, no. 10, p. 850, 2022, https://doi.org/10.3390/machines10100850.

[68] F. Aminifar, M. Abedini, T. Amraee, P. Jafarian, M. H. Samimi and M. Shahidehpour, "A review of power system protection and asset management with machine learning techniques," *Energy Systems*, vol. 13, pp. 855–892, 2022, https://doi.org/10.1007/s12667-021-00448-6.

[69] M. Hasan *et al*., "A critical review on control mechanisms, supporting measures, and monitoring systems of microgrids considering large scale integration of renewable energy sources," *Energy Reports*, vol. 10, pp. 4582–4603, 2023, https://doi.org/10.1016/j.egyr.2023.11.025.

[70] D. Dhinakaran, S. M. Udhaya Sankar, B. C. Latha, A. E. J. Anns and V. K. Sri, "Dam Management and Disaster Monitoring System using IoT," *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, pp. 1197-1201, 2023, https://doi.org/10.1109/ICSCDS56580.2023.10105132.

[71] V. Bolgouras, T. Ioannidis, I. Politis, A. Zarras and C. Xenakis, "Retina: Distributed and secure trust management for smart grid applications and energy trading," *Sustainable Energy, Grids and Networks*, vol. 38, p. 101274, 2024, https://doi.org/10.1016/j.segan.2024.101274.

[72] Y. Alghofaili and M. A. Rassam, "A trust management model for iot devices and services based on the multi-criteria decision-making approach and deep long short-term memory technique," *Sensors*, vol. 22, no. 2, p. 634, 2022, https://doi.org/10.3390/s22020634.

[73] L. Wei, Y. Yang, J. Wu, C. Long and B. Li, "Trust Management for Internet of Things: A Comprehensive Study," in *IEEE Internet of Things Journal*, vol. 9, no. 10, pp. 7664-7679, 2022, https://doi.org/10.1109/JIOT.2021.3139989.

[74] E. Alalwany and I. Mahgoub, "Security and trust management in the internet of vehicles (iov): Challenges and machine learning solutions," *Sensors*, vol. 24, no. 2, p. 368, 2024, https://doi.org/10.3390/s24020368.

[75] Y. Yan, "The overview of elliptic curve cryptography (ecc)," in *Journal of Physics: Conference Series*, vol. 2386, no. 1, p. 012019, 2022, https://doi.org/10.1088/1742-6596/2386/1/012019.

[76] K. Javeed, A. El-Moursy and D. Gregg, "EC-Crypto: Highly Efficient Area-Delay Optimized Elliptic Curve Cryptography Processor," in *IEEE Access*, vol. 11, pp. 56649-56662, 2023, https://doi.org/10.1109/ACCESS.2023.3282781.

[77] A. Yadav, P. Sharma and Y. Gigras, "A Comparative Study of Elliptic curve and Hyperelliptic Curve Cryptography Methods and an Overview of Their Applications," *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, pp. 01-06, 2024, https://doi.org/10.1109/ISCS61804.2024.10581015.

[78] A. Sebbah and K. Benamar, "A privacy-enhanced scheme within the public key infrastructure for the internet of things, employing elliptic curve diffie-hellman (ecdh)," *Indonesian Journal of Electrical Engineering and Informatics (IJEEI)*, vol. 12, no. 1, pp. 65–74, 2024, http://dx.doi.org/10.52549/ijeei.v12i1.5392.

[79] H. H. Hadi and A. A. Neamah, "An image encryption method based on modified elliptic curve diffie-hellman key exchange protocol and hill cipher," *Open Engineering*, vol. 14, no. 1, p. 20220552, 2024, https://doi.org/10.1515/eng-2022-0552.

[80] Z. A. Abduljabbar, V. O. Nyangaresi and J. Ma, *Mac-based symmetric key protocol for secure*, Springer Nature, 2022, https://books.google.co.id/books?id=gBuKEAAAQBAJ&hl=id&source=gbs_navlinks_s.

[81] D. Wang, A. Maximov, P. Ekdahl, and T. Johansson, "A new stand-alone mac construct called smac," *IACR Transactions on Symmetric Cryptology*, vol. 2025, no. 1, pp. 5–43, 2025, https://doi.org/10.46586/tosc.v2025.i1.5-43.

[82] C. W. Chuah, J. Alawatugoda, and N. Arbaiy, "On constructing a secure and fast key derivation function based on stream ciphers," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 16, p. 1486, 2024, https://doi.org/10.14569/ijacsa.2024.01506148.

[83] O. Italis, S. Pierre, and A. Quintero, "Privacy-preserving model for biometric-based authentication and key derivation function," *Journal of Information Security and Applications*, vol. 78, p. 103624, 2023, https://doi.org/10.1016/j.jisa.2023.103624.